UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

-v-

WILFREDO SEPULVEDA,

Defendant.

No. 18-cr-363 (RJS)
ORDER

RICHARD J. SULLIVAN, Circuit Judge:

Now before the Court is Defendant Wilfredo Sepulveda's motion to suppress electronic evidence recovered by government agents following the search of Defendant's iPhone pursuant to a search warrant issued by Magistrate Judge Lehrburger on June 4, 2018. Specifically, Defendant argues that (1) probable cause did not support the search warrant; (2) the warrant was overbroad and not sufficiently particularized; and (3) the manner in which the search was conducted exceeded the scope of the warrant. (Doc. Nos. 14, 26, 31, 38, 47.) With respect to his third argument, Defendant alternatively requests a hearing on the issue of how the iPhone search was conducted. (Doc. Nos. 14, 31, 38, 47.) At the oral argument on January 22, 2019, the Court ruled that probable cause supported the warrant and reserved decision on Defendant's remaining arguments. For the reasons set forth below, and as stated on the record at oral argument with respect to the probable cause issue, Defendant's motion to suppress and request for a hearing are denied.[1]

[1] In deciding this motion, the Court has considered the parties' written submissions (Doc. Nos. 14, 25, 26, 31, 32, 38, 43, 47), the transcript of the January 22, 2019 oral argument ("Tr."), the government's exhibit ("GX-1") (declaration of Detective Steven Saint-Hilaire), Defendant's

I. BACKGROUND

On May 15, 2018, the government filed a complaint charging Defendant with Hobbs Act robbery, in violation of 18 U.S.C. § 1951; possession of a controlled substance with intent to distribute, in violation of 21 U.S.C. § 841(a)(1) and (b)(1)(B); and use of a firearm during or in relation to a crime of violence or drug trafficking, in violation of 18 U.S.C. § 924(c)(1)(A)(ii).[2] (Doc. No. 1.) As relevant to those charges, the government alleges that Defendant stole cash and cocaine from a narcotics stash house in the Bronx on May 14, 2018. (*Id.*)

On June 4, 2018, Special Agent Tyler Myceli applied for a warrant to search and seize electronically stored information ("ESI") on two cell phones, one an iPhone and the other a flip phone, which law enforcement personnel recovered from Defendant around the time of his arrest. (DX-A.) Magistrate Judge Lehrburger signed the warrant the same day (DX-B), and investigators began executing it on or about June 7, 2018 (*see* GX-1 at 3). The search of the flip phone did not yield responsive ESI, but investigators discovered such ESI on the iPhone in the form of messages and photos sent, received, or taken between February 1, 2018 and May 23, 2018. (GX-1 at 3, 7.)

A. The Affidavit and Search Warrant

In support of his application for the search warrant, Agent Myceli submitted an affidavit

---

exhibits ("DX-_"), the supplemental declaration of Detective Saint-Hilaire ("S-H Supp. Decl."), and the declarations of Special Agents Seth Mastropaolo ("Mastropaolo Decl.") and Michael Medlin ("Medlin Decl.").

[2] A grand jury subsequently returned an indictment on May 22, 2018 charging Defendant with the same crimes. (Doc. No. 5.) On February 21, 2019, the grand jury returned a third superseding indictment charging Defendant with the same Hobbs Act robbery and firearm offenses, as well as two counts of possession of a controlled substance with intent to distribute, in violation of 21 U.S.C. § 841(a)(1) and (b)(1)(A), and one count of being a felon in possession of a firearm, in violation of 18 U.S.C. § 922(g). (Doc. No. 48.)

stating that, in addition to the May 2018 robbery charged in this case, Defendant also engaged in a home invasion robbery two months earlier, on February 9, 2018. (DX-A at 3.) Specifically, the affidavit stated that video footage showed Defendant at the scene of the February robbery "using what appears to be an iPhone." (DX-A at 7.) The affidavit further stated that, prior to the May 2018 robbery, video footage showed Defendant wearing a wig and dress while "using [t]he iPhone's camera to look at himself" at the scene of the robbery. (*Id.*)

With respect to search procedures, the affidavit requested that law enforcement personnel be permitted to search the iPhone for responsive ESI "sent, received, or obtained from the period of February 1, 2018 to March 23, 2018." (*Id.* at 8.) The affidavit also provided several illustrative techniques to be employed by law enforcement personnel, including a keyword search and "a file-by-file review [that entailed] 'opening' or reading the first few 'pages' of such files in order to determine their precise contents." (*Id.*) The affidavit further stated that law enforcement personnel would make "reasonable efforts to restrict their search to data falling within the categories specified in the warrant." (*Id.* at 9.) The affidavit nevertheless indicated that, "[d]epending on the circumstances, . . . law enforcement may need to conduct a complete review of all the ESI from the Subject Device to locate all data responsive to the warrant." (*Id.*)

The search warrant did not incorporate or attach the Myceli affidavit. (*See* DX-B.) The warrant did, however, attach a list of nine categories of ESI that law enforcement personnel were authorized to review ("Attachment A"). (*Id.* Att. A.) As relevant here, category six consisted of "text, data, chat, digital photographs[,] and video" as well as messages and any associated attachments or information pertaining to the robberies or narcotics; category eight consisted of "bank records, checks, credit card bills, account information, and other financial records"; and category nine consisted of "[e]vidence of user attribution showing who used or owned the

Subject Device at the time the records and items described in the warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history." (*Id.*)

B. Execution of the Warrant

In July 2018, Special Agent Seth Mastropaolo of the Bureau of Alcohol, Tobacco, Firearms, and Explosives ("ATF") sent Defendant's locked iPhone to the ATF's Digital Forensics Branch, along with the signed search warrant. (Mastropaolo Decl. at 2; Medlin Decl. at 2.) The Digital Forensics Branch successfully used a program called GrayKey to determine the iPhone's password. (Medlin Decl. at 2.) As part of that process, GrayKey automatically generated a partial extraction of the iPhone. (*Id.* at 2.)

The Digital Forensics Branch next sent the iPhone and partial extraction back to Mastropaolo, who then generated a searchable report of the partial extraction. (Mastropaolo Decl. at 2; Medlin Decl. at 2.) Mastropaolo, in turn, sent the partial extraction report to NYPD Detective Steven Saint-Hilaire, who reviewed it and, "finding it apparently incomplete," requested a full extraction. (S-H Supp. Decl. at 3; Mastropaolo Decl. at 2.) Using a Cellebrite data extraction program, Mastropaolo extracted a "full forensic copy of the iPhone's data" (the "Extracted iPhone") and provided it to Saint-Hilaire. (S-H Supp. Decl. at 3; Mastropaolo Decl. at 2.)

Before searching the Extracted iPhone, Saint-Hilaire reviewed the search warrant and affidavit. (S-H Supp. Decl. at 3.) Saint-Hilaire also spoke with AUSA Kyle Wirshba. (*Id.* at 3–4.) Although the search warrant did not expressly include a date range for responsive ESI or incorporate or attach the Myceli affidavit (which did include such a date range), Wirshba instructed Saint-Hilaire that he had authorization to search for responsive ESI only within the

affidavit's date range, which was from February 1, 2018 to March 23, 2018. (*Id.*; DX-A at 8.)

Saint-Hilaire proceeded to search the Extracted iPhone for messages, call logs, contacts, and photographs within that range. (S-H Supp. Decl. at 4.) With respect to photographs, however, the Extracted iPhone displayed "thumbnail" versions that initially appeared undated. (*Id.* at 5.) Consistent with his understanding of the search warrant authorization, Saint-Hilaire clicked on every thumbnail, which then displayed the date the photographed was created, to determine if any photographs were responsive. (*Id.*) Although Cellebrite software allowed Saint-Hilaire to restrict his search of photographs to a date range without viewing every photograph on the phone, he was unaware of that search function until after the search was over. (*Id.* at 6.) Ultimately, Saint-Hilaire identified four responsive photographs, each of which fell within the date range in the Myceli affidavit. (*Id.*)

II. Applicable Law

The Fourth Amendment of the United States Constitution provides in relevant part that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. In other words, "a warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity." *Kentucky v. King*, 563 U.S. 452, 459 (2011). Further, "because a warrant generally authorizes no more than what it expressly provides, to act unreasonably beyond the terms of a warrant is akin to acting without a warrant at all." *Simon v. City of New York*, 893 F.3d 83, 94 (2d Cir. 2018).

A defective warrant or search, however, does not necessarily require suppression of evidence. Under the so-called "good faith exception" to the exclusionary rule, suppression is not warranted where the government demonstrates the "objective reasonableness of the officers'

good faith reliance" on a warrant, *United States v. Clark*, 638 F.3d 89, 100 (2d Cir. 2011) (quoting *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992)), even if the warrant is constitutionally defective, *see United States v. Ganias*, 824 F.3d 199, 221 (2d Cir. 2016) (en banc). Thus, in the case of searches conducted pursuant to a warrant, the good faith "exception" is perhaps better characterized as the rule, since "most searches [so] conducted . . . would likely fall within its protection." *Clark*, 638 F.3d at 100; *see also Herring v. United States*, 555 U.S. 135, 140 (2009) ("[E]xclusion has always been our last resort, not our first impulse . . . ." (internal quotation marks omitted)).

Nevertheless, the Second Circuit has determined that the good faith exception does not apply

> (1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable.

Clark, 638 F.3d at 100 (quoting *United States v. Moore*, 968 F.2d 216, 222 (2d Cir. 1992)). Of course, "[n]ot every facially deficient warrant . . . will be so defective that an officer will lack a reasonable basis for relying upon it." *United States v. Rosa*, 626 F.3d 56, 66 (2d Cir. 2010). Although the Court may not "rely on unincorporated, unattached supporting documents to cure a constitutionally defective warrant, those documents are still relevant to [the] determination of whether the officers acted in good faith, because they contribute to [the Court's] assessment of the officers' conduct in a particular case." *Id.* at 64. Finally, in considering whether the good faith exception applies, the Court must make "the additional determination that the officers' conduct was sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* at 66 (internal

quotation marks and citation omitted).

III. Discussion

The Court will address Defendant's arguments regarding overbreadth, particularity, and the manner of the search in turn.

A. Overbreadth

"[A]n otherwise unobjectionable description of the objects to be seized" or searched "is defective if it is broader than can be justified by the probable cause upon which the warrant is based." *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013) (alterations in original) (quoting 2 W. LaFave, Search and Seizure § 4.6(a) (5th ed. 2012)). Therefore, "[i]n determining whether a warrant is overbroad, courts must focus on whether there exists probable cause to support the breadth of the search that was authorized." *United States v. Zemlyansky*, 945 F. Supp. 2d 438, 464 (S.D.N.Y. 2013) (internal quotation marks omitted).

Defendant argues that the warrant was facially overbroad with respect to certain categories of ESI listed in Attachment A. Specifically, Defendant focuses on categories eight (financial records) and nine (evidence of user attribution). (Tr. at 33–34.) Defendant asserts that there was no probable cause to show that he used any of the financial records listed in category eight, and that the user attribution category is essentially a catch-all that permits the type of rummaging that is proscribed by the Fourth Amendment. (*Id.* at 34–37.) The Court disagrees.

At the outset, the Court notes that it has already ruled, for the reasons stated on the record at the oral argument, that probable cause supported the search warrant with respect to Defendant's iPhone in general. (*See* Tr. at 28.) The Court is not persuaded that it should reconsider that ruling with respect to the financial records and user attribution categories set out in the warrant. As for the former category, it is entirely reasonable to believe that any electronic

financial records on Defendant's iPhone would contain evidence of the charged robbery offense. *See, e.g.*, *United States v. Robinson*, No. 16-cr-545-ADS, 2018 WL 5928120, at *18 (E.D.N.Y. Nov. 13, 2018). With respect to category nine, evidence of the iPhone user's identity in relation to the ESI already listed in the warrant was clearly relevant to the charged offense, and district courts have found probable cause to search a cell phone's user attribution data. *See, e.g.*, *United States v. Hassan*, No. 18-cr-26-PJS/SER, 2018 WL 2344452, at *4 (D. Minn. May 8, 2018), *R. & R. adopted*, 2018 WL 2342902 (D. Minn. May 23, 2018); *In re Black iPhone 4*, 27 F. Supp. 3d 74, 77–78 & n.7 (D.D.C. 2014).

Finally, even if it could be argued that the search warrant was overbroad, Defendant's motion would still fail since (1) law enforcement personnel did not find any financial records during the search, and thus there are no financial records to suppress (GX-1 at 7), and (2) the Myceli affidavit – which described video footage of Defendant's apparent use of an iPhone near two robberies – provided sufficient indicia of probable cause such that it was reasonable for investigators to rely on it in searching for any user attribution data on Defendant's iPhone. *See See Clark*, 638 F.3d at 100; *Rosa*, 626 F.3d at 66. Accordingly, the government has, at the very least, satisfied the good faith exception.

B. Particularity

Defendant next argues that the warrant was not sufficiently particularized because it failed to restrict the iPhone search to a specific date range. (Doc. No. 14 at 13; Tr. 44.) Although it is true that the affidavit's date range was never incorporated into the warrant, the Court concludes that the good faith exception applies and that such a date range – which was in fact adhered to by the government – was justified by the facts set forth in the affidavit.

Although Defendant is correct that several district courts in this Circuit have been critical

of warrants that failed to include a temporal limitation, *e.g.*, *United States v. Wey*, 256 F. Supp. 3d 355, 387 (S.D.N.Y. 2017); *United States v. Levy*, No. S5 11-cr-62-PAC, 2013 WL 664712, at *11 n.7 (S.D.N.Y. Feb. 25, 2013), *aff'd*, 803 F.3d 120 (2d Cir. 2015), none of these cases establishes a "binding principle of law sufficient to undermine an agent's good faith reliance on a . . . warrant," *United States v. Raymonda*, 780 F.3d 105, 119 (2d Cir. 2015). As one district court in this Circuit has concluded, "[i]n these circumstances, it cannot be said that executing officers should have realized a lack of date limitation constituted a facial deficiency in the Search Warrant such that reliance on it would be unreasonable." *Levy*, 2013 WL 664712, at *11. Thus, the Court concludes that the lack of a date limitation in the warrant does not require suppression, particularly since investigators complied the affidavit's date range, which was itself reasonable and supported by probable cause. *See Clark*, 638 F.3d at 100; *Rosa*, 626 F.3d at 66. Accordingly, any particularity violation does not require suppression.

C. The Manner of the Search

Finally, Defendant argues that government agents acted beyond the scope of the warrant by extracting a full copy of the iPhone's data and opening all photographs on the iPhone. In the alternative, Defendant requests a hearing on how the iPhone search was conducted. For the reasons that follow, the Court concludes that the investigators acted in good faith when extracting a full copy of the iPhone's data and when searching through the photographs stored on the iPhone. The Court further concludes that there is no issue of fact warranting a hearing.

1. Extraction of the iPhone's Data

It is an open question whether the mere copying of an electronic device to preserve its original content as a precursor for the search itself amounts to a search or seizure under the Fourth Amendment. *United States v. Loera*, 333 F. Supp. 3d 172, 185 (E.D.N.Y. 2018)

(collecting cases). The Court need not resolve this issue, however, because the good faith exception once again clearly applies.

Assuming without deciding that the copying of Defendant's iPhone amounted to a search or seizure that was not authorized by the warrant, such conduct is markedly different from objectively unreasonable police conduct. For example, in *United States v. Voustianiouk*, the Second Circuit held that officers who searched a second-floor apartment in a two-story building, when the warrant authorized only a search of the first-floor apartment, did not act in objectively reasonable reliance on that warrant. 685 F.3d 206, 215 (2d Cir. 2012). While recognizing that suppression of evidence was a "last resort" rather than a "first impulse," *id.* (quoting *Herring*, 555 U.S. at 140), the court concluded that suppression was necessary to deter similar police misconduct, *id.* at 217.

By contrast, courts have generally endorsed the routine law enforcement practice of copying a computer hard drive or cell phone data before conducting a search. *See, e.g.*, *United States v. Veloz*, 109 F. Supp. 3d 305, 313 (D. Mass. 2015) ("[T]he creation of a mirror image of a suspect computer hard drive for later analysis has become a common and constitutionally permissible practice."). The Second Circuit has recognized the valid reasons that support this practice: "Preservation of the original medium or a complete mirror may . . . be necessary in order to safeguard the integrity of evidence that has been lawfully obtained or to authenticate it at trial." *Ganias*, 824 F.3d at 215. In addition, "[r]etention of the original storage medium or its mirror may also be necessary to afford criminal defendants access to that medium or its forensic copy so that, relying on forensic experts of their own, they may challenge the authenticity or reliability of evidence allegedly retrieved." *Id.* Thus, "courts have routinely upheld the seizure and copying of hard drives and other storage devices in order to effectuate a proper search for the

categories of documents or files listed in a warrant." *United States v. Alston*, No. 15-cr-435-CM, 2016 WL 2609521, at *6 (S.D.N.Y. Apr. 29, 2016) (internal quotation marks omitted).

The Court finds that the law enforcement officials in this case simply adhered to the generally-accepted practice of creating a digital copy before conducting a search. Mastropaolo, the agent who created the full copy of Defendant's iPhone, stated that he "did a full extraction of the iPhone through the Cellebrite UFED Physical Analyzer" and uploaded the copied data to a hard drive that he gave to investigators. (Mastropaolo Decl. 2.) He further stated that he did not review any content on the iPhone. (*Id.*) Saint-Hilaire stated that he then "alone conducted a review of the Extracted iPhone" in accordance with the warrant and affidavit. (S-H Supp. Decl. at 3.) In short, nothing suggests that the investigators in this case created or used the extracted version of Defendant's iPhone in an objectively unreasonable manner. Accordingly, the good faith exception protects the investigators' extraction of data from Defendant's iPhone.

2. Search of Photographs on Defendant's iPhone

Defendant also argues that Saint-Hilaire exceeded the scope of the warrant by opening every photograph on Defendant's iPhone to determine which ones were responsive. (Doc. No. 38 at 3–4.) Defendant does not, however, dispute that the four responsive photographs that Saint-Hilaire discovered using that method fall within the terms of the warrant and the date range in the application. (*See id.* at 4.) Therefore, even assuming that Saint-Hilaire's search method was improper, the Court must still consider whether wholesale suppression of the fruits of the improper search is appropriate. "Government agents flagrantly disregard the terms of a warrant so that wholesale suppression is required only when (1) they effect a widespread seizure of items that were not within the scope of the warrant, and (2) do not act in good faith." *United States v. Shi Yan Liu*, 239 F.3d 138, 140 (2d Cir. 2000) (internal quotation marks and citations omitted).

The Court concludes that Saint-Hilaire acted in good faith, and thus wholesale suppression is not appropriate.

First, Defendant cannot point to any controlling precedent that prohibits a file-by-file search method. Indeed, the Second Circuit has declined to require "specific search protocols or minimization undertakings as basic predicates for upholding digital search warrants." *Galpin*, 720 F.3d at 451. Against this backdrop, district courts in this Circuit have regularly held file-by-file searches to be reasonable. *See, e.g.*, *United States v. Lustyik*, 57 F. Supp. 3d 213, 229 (S.D.N.Y. 2014); *United States v. Graziano*, 558 F. Supp. 2d 304, 317 (E.D.N.Y. 2008); *see also United States v. Fumo*, No. 06-cr-319, 2007 WL 3232112, at *6 (E.D. Pa. Oct. 30, 2007) ("Regardless of the search protocols or keywords used by the government, the government may open and briefly examine each computer file to determine whether it is within the description recited in the warrant."). The Court agrees with these decisions and adopts their reasoning.

Furthermore, Saint-Hilaire stated that he would have restricted his review of the iPhone's photographs to the relevant date range, as he did with other categories of ESI, but for the fact that he mistakenly believed such a search function did not exist with respect to the photographs. (S-H Supp. Decl. at 6.) Despite Defendant's skepticism, the Court finds no reason to disbelieve Saint-Hilaire's statement. Therefore, even if a less intrusive search method was available, Saint-Hilaire's conduct was not sufficiently deliberate such that the deterrent effect of suppression would be appropriate. *See Rosa*, 626 F.3d at 66. For these reasons, the Court concludes that Saint-Hilaire did not flagrantly disregard the terms of the search warrant, and that wholesale suppression of the responsive photographs is not appropriate.

3. Defendant's Alternative Request for a Hearing

After the government submitted declarations from its agents in response to the Court's

Order of January 22, 2019 (Doc. No. 33), Defendant renewed his request for a hearing on how the iPhone search was conducted (Doc. No. 38). Specifically, Defendant seeks an opportunity to cross-examine Saint-Hilaire as to his search methods. (*Id.* at 5.) Having now received two declarations from Detective Saint-Hilaire and one declaration each from Agents Mastropaolo and Medlin, the Court finds that there are no issues of fact that require an evidentiary hearing. Accordingly, Defendant's request for a hearing is denied.

IV. CONCLUSION

In sum, the Court holds that there was probable cause for the search warrant of Defendant's iPhone, and that to the extent there were deficiencies in the warrant issued by Judge Lehrburger, the government has met its burden of demonstrating the objective reasonableness of Saint-Hilaire's good faith reliance on the warrant. Accordingly, Defendant's motion to suppress and request for a hearing are DENIED, and the Clerk is respectfully directed to terminate the motion pending at docket number 14.

Trial in this matter will commence on Monday, March 18, 2019 at 9:30 a.m. in Courtroom 905, Thurgood Marshall United States Courthouse, 40 Foley Square, New York, New York 10007. As stated in the Court's Order of January 23, 2019 (Doc. No. 34), the parties shall appear for a final pretrial conference on Thursday, March 14, 2019 at 10:00 a.m., at which the Court will hear argument on all pending motions *in limine* and otherwise discuss the trial.

SO ORDERED.

Dated: March 4, 2019
New York, New York

RICHARD J. SULLIVAN
UNITED STATES CIRCUIT JUDGE
Sitting by Designation